

中华人民共和国国家标准

GB/T 43848—2024

网络安全技术 软件产品开源代码安全 评价方法

Cybersecurity technology—Evaluation method for open source code
security of software products

2024-04-25 发布

2024-11-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 概述 1

5 评价要素 2

5.1 评价参数 2

5.2 开源代码来源 3

5.2.1 概述 3

5.2.2 开源代码规模与占比 3

5.2.3 开源代码编码语言 3

5.2.4 开源代码著作权人 3

5.2.5 开源代码贡献量 3

5.2.6 开源代码丰富度 3

5.2.7 开源社区安全管理 3

5.2.8 开源代码托管平台 3

5.2.9 开源代码下载平台 3

5.3 开源代码安全质量 4

5.3.1 概述 4

5.3.2 开源代码漏洞率 4

5.3.3 开源代码漏洞严重性 4

5.3.4 开源代码漏洞修复率 4

5.3.5 开源代码版本更新情况 4

5.4 开源代码知识产权 4

5.4.1 概述 4

5.4.2 开源许可证遵从度 4

5.4.3 开源许可证规范性 4

5.4.4 开源许可证互惠性 4

5.4.5 开源许可证兼容性 4

5.4.6 开源许可证专利情况 4

5.4.7 开源许可证适用范围 5

5.5 开源代码管理 5

5.5.1 概述 5

5.5.2	开源代码管理团队	5
5.5.3	开源代码物料清单	5
5.5.4	开源代码设计	5
5.5.5	开源代码生成	5
6	评价流程	5
6.1	概述	5
6.2	开源代码来源评价流程	5
6.2.1	开源代码规模与占比	5
6.2.2	开源代码编码语言	6
6.2.3	开源代码著作权人	6
6.2.4	开源代码贡献量	6
6.2.5	开源代码丰富度	6
6.2.6	开源社区安全管理	6
6.2.7	开源代码托管平台	6
6.2.8	开源代码下载平台	6
6.3	开源代码安全质量评价流程	7
6.3.1	开源代码漏洞率	7
6.3.2	开源代码漏洞严重性	7
6.3.3	开源代码漏洞修复率	7
6.3.4	开源代码版本更新情况	7
6.4	开源代码知识产权评价流程	7
6.4.1	开源许可证遵从度	7
6.4.2	开源许可证规范性	8
6.4.3	开源许可证互惠性	8
6.4.4	开源许可证兼容性	8
6.4.5	开源许可证专利情况	8
6.4.6	开源许可证适用范围	8
6.5	开源代码管理评价流程	8
6.5.1	开源代码管理团队	8
6.5.2	开源代码物料清单	8
6.5.3	开源代码设计	8
6.5.4	开源代码生成	9
附录 A (资料性)	开源代码安全风险	10
A.1	开源网络安全风险	10
A.2	开源知识产权风险	10
A.3	开源持续性风险	10
参考文献		11

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国信息通信研究院、蚂蚁科技集团股份有限公司、华为技术有限公司、中兴通讯股份有限公司、山东浪潮科学研究院有限公司、阿里云计算有限公司、深信服科技股份有限公司、腾讯云计算(北京)有限责任公司、杭州默安科技有限公司、深圳开源互联网安全技术有限公司、北京百度网讯科技有限公司、深圳市腾讯计算机系统有限公司、北京天融信网络安全技术有限公司、奇安信网神信息技术(北京)股份有限公司、浪潮电子信息产业股份有限公司、北京小米移动软件有限公司、北京京东尚科信息技术有限公司、北京金山云网络技术有限公司、北京火山引擎科技有限公司、恒安嘉新(北京)科技股份公司、启明星辰信息技术集团股份有限公司、用友网络科技股份有限公司、杭州安恒信息技术股份有限公司、北京知道创宇信息技术股份有限公司、长扬科技(北京)股份有限公司、星环信息科技(上海)股份有限公司、浙江大华技术股份有限公司、超聚变数字技术有限公司、美的集团股份有限公司、马上消费金融股份有限公司、泰康保险集团股份有限公司、道普信息技术有限公司、中电科网络安全科技股份有限公司、国网区块链科技(北京)有限公司、北京安普诺信息技术有限公司、中国信息安全测评中心、中国软件评测中心、中电科拟态安全技术有限公司、杭州孝道科技有限公司、北京珞安科技有限责任公司、深圳华大生命科学研究院、兴唐通信科技有限公司、墨菲未来科技(北京)有限公司、北京酷德啄木鸟信息技术有限公司、中国科学院软件研究所、中国网络空间研究院、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、中国科学院信息工程研究所、浙江省电子信息产品检验研究院、中国电子信息产业集团有限公司第六研究所、博鼎实华(北京)技术有限公司、ABB(中国)有限公司、三六零科技集团有限公司、北京神州绿盟科技有限公司、西安交大捷普网络科技有限公司、深圳市能信安科技股份有限公司、联想(北京)有限公司、北京长亭未来科技有限公司、北京山石网科信息技术有限公司、广东云百科技有限公司、武汉安天信息技术有限责任公司、北京智游网安科技有限公司、北京九章云极科技有限公司、麒麟软件有限公司、新华三技术有限公司、天翼云科技有限公司、OPPO 广东移动通信有限公司。

本文件主要起草人：栗蔚、郭雪、李晓明、吴江伟、程岩、白晓媛、崔锦国、高琨、张锐刚、项曙明、李响、魏子重、方强、曾林青、赵振阳、叶润国、郑剑锋、沈锡镛、孟瑾、聂万泉、王颀、郭建领、代威、杨剑、董国伟、曹柱、钱佳煜、李欣博、李晓川、张志文、李鹏超、赵军凯、季晟宇、袁明坤、周景平、范雷、刘汪根、张剑青、惠静、张亮亮、刘志强、安丙春、韩明军、王会波、杨珂、张涛、王晓萌、袁薇、侯大鹏、谢国苗、延鹏、蔡国瑜、郝高健、欧阳强斌、史明超、晏敏、姜伟、吴巍、吴倩、刘楠、许丽丽、尹肖栋、王绍杰、董霁、王缀、张杰、张帆、何建锋、李德庆、刘俊、翟羽佳、荣钰、刘超、余丽娜、韩云、方磊、刘敏、万晓兰、洪钧煌、朱丽亚。

网络安全技术 软件产品开源代码安全 评价方法

1 范围

本文件规定了软件产品中的开源代码成分安全评价要素和评价流程。

本文件适用于对软件产品包含的开源代码成分进行静态安全评价,为各单位对于软件产品中的开源代码成分进行安全性自评价提供依据,为第三方机构开展此类工作提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2022 信息安全技术 术语

3 术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

软件产品 software product

计算机软件、信息系统或设备中嵌入的软件,或在提供计算机信息系统集成、应用等技术服务时提供的计算机软件,表现形式为一组计算机代码、规程以及可能的相关文档和数据。

[来源:GB/T 36475—2018,3.1,有修改]

3.2

开源代码 open source code

公众可以获取源代码的计算机代码。

注:其著作权人通过开源许可证将代码的复制、修改、再发布的权利向公众开放。

3.3

开源许可证 open source license

允许公众用户根据协议内容使用、修改、复制和分发开源代码的授权协议。

3.4

开源社区 open source community

以开源代码的贡献者为主体,在开源代码贡献过程中形成的具有特定文化、组织结构、运行机制的共同体。

4 概述

当前开源代码被广泛应用在软件产品时,存在开源代码网络安全风险、知识产权风险和持续性风险(见附录 A)。

软件产品开源代码安全评价方法包含评价要素和评价流程。其中,评价要素覆盖开源代码来源、开源代码安全质量、开源代码知识产权和开源代码管理,评价流程依据评价要素给出评价过程与手段。

对软件产品包含的开源代码进行安全评价,有利于达到以下目的。

- a) 可控性:通过评价软件产品中开源代码编码语言、贡献量、丰富度等开源代码来源情况,掌握开源代码供应中断风险的情况,实现对可控性的判断。
- b) 安全性:通过考察软件产品中开源代码安全漏洞率、版本更新等情况,掌握开源代码网络安全事件发生可能性的情况,实现对安全性的判断。
- c) 合规性:通过考察软件产品中开源代码开源许可证互惠性、兼容性等情况,掌握开源许可证知识产权风险的情况,实现对合规性的判断。
- d) 稳定性:通过考察软件产品中开源代码管理团队、开源代码物料清单等情况,掌握软件产品整体应对开源代码网络安全风险、知识产权风险和持续性风险的情况,实现对稳定性的判断。

5 评价要素

5.1 评价参数

评价参数体系由开源代码来源、开源代码安全质量、开源代码知识产权、开源代码管理四个方面的两级参数构成,具体见表 1。

表 1 软件产品包含的开源代码安全评价参数

一级参数	二级参数
开源代码来源	开源代码规模与占比
	开源代码编码语言
	开源代码著作权人
	开源代码贡献量
	开源代码丰富度
	开源社区安全管理
	开源代码托管平台
	开源代码下载平台
开源代码安全质量	开源代码漏洞率
	开源代码漏洞严重性
	开源代码漏洞修复率
	开源代码版本更新情况
开源代码知识产权	开源许可证遵从度
	开源许可证规范性
	开源许可证互惠性
	开源许可证兼容性
	开源许可证专利情况
	开源许可证适用范围

表 1 软件产品包含的开源代码安全评价参数（续）

一级参数	二级参数
开源代码管理	开源代码管理团队
	开源代码物料清单
	开源代码设计
	开源代码生成

5.2 开源代码来源

5.2.1 概述

此类参数主要掌握软件产品中开源代码来源情况,实现对其可控性的判断。

5.2.2 开源代码规模与占比

统计软件产品包含的各开源代码模块字节数规模及其在软件产品代码中所占比例。

5.2.3 开源代码编码语言

统计软件产品包含的开源代码模块所使用的编码语言种类及其所开发代码占软件产品的比例。

5.2.4 开源代码著作权人

统计软件产品包含的各开源代码著作权人基本信息,包括名称、所在国家或地区、所属组织、贡献承诺签署情况等。

5.2.5 开源代码贡献量

统计软件产品包含的开源代码参与者的贡献量情况,包括但不限于:

- a) 各开源代码贡献者贡献代码量及占比;
- b) 开源代码维护者情况,包括翻译、测试、活动组织等。

5.2.6 开源代码丰富度

统计软件产品包含的开源代码在功能等方面具有可更换的其他代码(含开源或商业代码)情况。

5.2.7 开源社区安全管理

统计软件产品包含的开源代码所依赖的开源社区安全管理情况,包括但不限于:

- a) 统计开源社区对于开源代码的安全扫描情况;
- b) 统计开源社区对于开源代码的贡献管理,如签署开源贡献协议、具备代码审查机制、具备数字签名。

5.2.8 开源代码托管平台

统计软件产品包含的开源代码托管平台运营方基本信息。

5.2.9 开源代码下载平台

统计软件产品包含的开源代码下载平台运营方情况,包括但不限于:

- a) 统计软件产品包含的开源代码下载平台运营方基本信息；
- b) 统计开源代码下载平台对开源代码完整性的保障情况。

5.3 开源代码安全质量

5.3.1 概述

此类参数主要掌握软件产品中开源代码安全质量情况,实现对其安全性的判断。

5.3.2 开源代码漏洞率

统计软件产品包含的开源代码模块的原始漏洞数量和千行漏洞率情况。

5.3.3 开源代码漏洞严重性

参考 GB/T 30279—2020 中 6.3.3 统计软件产品包含的开源代码模块原始漏洞严重性。

5.3.4 开源代码漏洞修复率

统计软件产品包含的开源代码已修复漏洞在其所有发现的漏洞中的占比及修复时间。

5.3.5 开源代码版本更新情况

统计软件产品包含的开源代码所用版本与开源社区最新发布版本相比的滞后情况。

5.4 开源代码知识产权

5.4.1 概述

此类参数主要掌握软件产品中开源代码知识产权情况,实现对合规性的判断。

5.4.2 开源许可证遵从度

统计软件产品包含的开源代码履行开源许可证规定的相关条款、义务情况。

5.4.3 开源许可证规范性

统计软件产品包含的开源代码对应许可证编写规范性情况,评价内容涉及授权范围、授权条件、违约与授权终止、免责声明等。

5.4.4 开源许可证互惠性

统计软件产品包含的开源代码是否存在互惠性开源许可证(即许可证明确需分发修改后的源码)并采取对应处置措施的情况。软件产品应对所涉及的自由互惠开源许可证进行识别和风险评估,判断自研代码与开源代码之间的合规使用情况。

5.4.5 开源许可证兼容性

统计软件产品包含的开源代码所使用的各开源许可证之间兼容性情况,以判断软件产品对开源许可证合规使用情况。

5.4.6 开源许可证专利情况

统计软件产品包含的开源代码所使用的开源许可证是否明确专利授权情况。

5.4.7 开源许可证适用范围

统计软件产品包含的开源代码所使用的开源许可证的适用范围和出现纠纷时法律声明情况。

5.5 开源代码管理

5.5.1 概述

此类参数主要掌握软件产品中开源代码管理情况,实现对稳定性的判断。

5.5.2 开源代码管理团队

评价软件产品包含的开源代码的管理团队完善程度,内容包括但不限于:

- a) 建立管理团队对开源代码进行统一管控,并进行相应管理角色划分;
- b) 建立开源代码管理人员白名单和退出机制。

5.5.3 开源代码物料清单

评价软件产品包含的开源代码物料清单的完备性,包括建立和维护可追溯性的策略和程序,记录和保留开源代码的原始供应方、开源社区或开发贡献者等相关信息。

5.5.4 开源代码设计

评价软件产品包含的开源代码设计文档完备性,以及梳理开源代码兼容性、使用规范性情况。

5.5.5 开源代码生成

评价软件产品程序的源代码编写完成后,在编译以及链接过程中对使用的开源代码采取的安全措施,包括配置检查、漏洞扫描等,达到代码生成安全。

6 评价流程

6.1 概述

评价实施方依据国家相关规定,主要对软件产品中的开源代码来源、开源代码安全质量、开源代码知识产权和开源代码管理进行评价。

评价实施方在开展开源代码安全评价工作中应综合采用访谈、检查和测试等基本评价流程,以核实被评价单位所提供评价材料是否满足指标考查内容要求。

- a) 访谈:评价实施方通过与被评价单位相关人员进行有针对性的交流以帮助理解、厘清或取得证据,访谈的对象为个人或团体,如技术团队负责人、核心技术工程师等。
- b) 检查:评价实施方对被评价单位提供的相关材料进行观察、查验、分析以帮助理解、厘清或取得证据,检查的对象为制度、文档和记录,如:必要的开源代码技术设计文档、安全扫描报告、开源代码管理团队背景信息等。
- c) 检测:评价实施方检测软件产品中未经改动的开源代码成分,形成开源代码清单列表;检测软件产品中未经改动的开源代码漏洞,形成开源代码漏洞检测报告。

6.2 开源代码来源评价流程

6.2.1 开源代码规模与占比

检测软件产品形成开源代码清单列表,检查各开源代码模块的规模大小及所占比例并进行记录。

6.2.2 源代码编码语言

源代码编码语言的评价流程如下：

- a) 检测软件产品形成源代码清单列表,检查各源代码模块的编码语言名称;
- b) 访谈软件研发相关人员获取软件产品研发常用编码语言信息。

6.2.3 源代码著作权人

源代码著作权人的评价流程如下：

- a) 检测软件产品形成源代码清单列表,检查各源代码模块的著作权人的地址信息、所在国家或地区、所属组织信息;
- b) 检测源代码形成源代码清单列表,检查各源代码模块的著作权人是否受战争、贸易管制、知识产权等一种或多种安全因素影响。

6.2.4 源代码贡献量

源代码贡献量的评价流程如下：

- a) 检测软件产品形成源代码清单列表,检查各源代码模块的贡献者地址信息、所在国家或地区和所属组织信息;
- b) 统计各贡献者合并代码次数占比;
- c) 检测软件产品形成源代码清单列表,检查各源代码模块的贡献者是否受战争、贸易管制、知识产权等一种或多种安全因素影响。

6.2.5 源代码丰富度

源代码丰富度的评价流程如下：

- a) 检测软件产品形成源代码清单列表,检查各源代码模块是否受战争、贸易管制、知识产权等一种或多种安全因素影响;
- b) 检测软件产品形成源代码清单列表,检查此类代码是否具备可更换的其他代码(含开源或商业)。

6.2.6 开源社区安全管理

开源社区安全管理的评价流程如下：

- a) 检测软件产品形成源代码清单列表,检查各源代码模块所依赖的开源社区声明文档是否定期发布安全问题;
- b) 检查各源代码模块所依赖的开源社区源代码合并是否具备安全测试标记;
- c) 检查各源代码模块所依赖的开源社区贡献规则文档,确认开源社区是否要求开源贡献者签署协议;
- d) 检查各源代码模块所依赖的开源社区组织架构,确认是否有专门的人员进行代码审查;
- e) 检查各源代码模块所依赖的开源社区的贡献代码列表,确认是否具备数字签名。

6.2.7 源代码托管平台

检测软件产品形成源代码清单列表,检查各源代码模块的代码托管平台运营方是否不受战争、贸易管制、知识产权等一种或多种安全因素影响。

6.2.8 源代码下载平台

源代码下载平台的评价流程如下：

- a) 检测软件产品形成开源代码清单列表,检查各开源代码模块的下载运营方是否不受战争、贸易管制、知识产权等一种或多种安全因素影响;
- b) 检查各开源代码模块的哈希值和数字签名;
- c) 检查各开源代码模块官网地址哈希值和数字签名,与软件产品使用的开源代码进行比对,判断软件产品使用的开源代码是否被篡改。

6.3 开源代码安全质量评价流程

6.3.1 开源代码漏洞率

开源代码漏洞率的评价流程如下:

- a) 检测软件产品形成开源代码漏洞检测报告,检查各开源代码模块是否存在已知漏洞;
- b) 检查开源代码中每千行的已知漏洞数量;
- c) 计算有漏洞的开源代码中平均漏洞个数。

6.3.2 开源代码漏洞严重性

开源代码漏洞严重性的评价流程如下:

- a) 将各已知漏洞的被利用性参数进行赋值,根据赋值结果,参考 GB/T 30279—2020 的附录 A 计算得出漏洞被利用性分级;
- b) 将已知漏洞的影响程度参数进行赋值,根据赋值结果,参考 GB/T 30279—2020 的附录 B 计算得到影响程度分级;
- c) 根据被利用性和影响程度分级的结果,参考 GB/T 30279—2020 的附录 D 计算得到安全漏洞分级结果;
- d) 检查软件产品包含的开源代码是否存在中危及以上漏洞;
- e) 统计软件产品包含的开源代码中危及以上漏洞占比。

6.3.3 开源代码漏洞修复率

开源代码漏洞修复率的评价流程如下:

- a) 检查软件产品包含的开源代码漏洞修复记录;
- b) 检查漏洞出现正式编号的时间;
- c) 检查修复记录中危及以上漏洞的平均修复时间是否超过 3 个月;
- d) 统计中危及以上漏洞的平均修复时间在 3 个月内的占比。

6.3.4 开源代码版本更新情况

开源代码版本更新情况的评价流程如下:

- a) 检测软件产品形成开源代码清单列表,检查各开源代码模块当前使用的版本发布时间;
- b) 检查各开源代码模块在开源社区中最新版本发布时间;
- c) 检查各开源代码模块是否为较新稳定版本,如 4 年内发布;
- d) 统计开源代码为较新稳定版本的占比。

6.4 开源代码知识产权评价流程

6.4.1 开源许可证遵从度

开源许可证遵从度的评价流程如下:

- a) 检测软件产品形成开源代码清单列表,检查各开源代码模块是否遵守开源许可证的相关要求;

- b) 统计软件产品中按照相关开源许可证要求规范使用的开源代码占比。

6.4.2 开源许可证规范性

检测软件产品形成开源代码清单列表,检查各开源许可证条款中是否包含授权范围、授权条件、违约与授权终止、免责声明等。

6.4.3 开源许可证互惠性

开源许可证互惠性的评价流程如下:

- a) 检测软件产品形成开源代码清单列表,检查开源代码中的弱互惠性开源许可证是否通过弱隔离方式引入,如静态链接和动态链接等;
- b) 检查开源代码中的强互惠性开源许可证是否通过强隔离方式引入,如聚合体。

6.4.4 开源许可证兼容性

检测软件产品形成开源代码清单列表,检查各开源代码模块的开源许可证之间是否兼容。

6.4.5 开源许可证专利情况

检测软件产品形成开源代码清单列表,检查各开源代码模块的开源许可证是否有明确专利授予。

6.4.6 开源许可证适用范围

检测软件产品形成开源代码清单列表,检查各开源代码模块的开源许可证适用范围是否为全球。

6.5 开源代码管理评价流程

6.5.1 开源代码管理团队

开源代码管理团队评价流程如下:

- a) 检查组织架构图,确认软件产品是否具备开源代码管理团队;
- b) 检查软件产品开源代码管理团队是否具备明确角色划分,覆盖对开源代码准入管理、供应商开源代码管理和开源代码的运维管理;
- c) 访谈软件产品团队人员获取人员从业经历情况,确认是否符合项目管理要求。

6.5.2 开源代码物料清单

开源代码物料清单的评价流程如下:

- a) 检查软件产品是否具备开源代码物料清单;
- b) 检查物料清单是否包含直接引入的开源代码原始供应方、开源社区或开发贡献者等基本信息;
- c) 检查物料清单是否包含间接依赖的开源代码原始供应方、开源社区或开发贡献者等基本信息;
- d) 检查软件产品包含的开源代码物料清单是否具备可追溯性。

6.5.3 开源代码设计

开源代码设计的评价流程如下:

- a) 检查软件产品是否具备开源代码部分的设计文档;
- b) 检查设计文档是否包含与运行环境兼容内容;
- c) 检查设计文档是否包含接口兼容和版本接口兼容内容。

6.5.4 开源代码生成

开源代码生成的评价流程如下：

- a) 检查软件产品在生成阶段是否具备开源代码部分的安全扫描报告；
- b) 检查软件产品包含的开源代码安全扫描策略配置是否合理。

附 录 A
(资料性)
开源代码安全风险

A.1 开源网络安全风险

开源网络安全风险是指由于源代码公开,资产直接暴露在互联网,在开源代码出现漏洞时容易被黑客读取,降低黑客攻击门槛导致代码安全性受到挑战。

A.2 开源知识产权风险

开源知识产权风险大致分为版权侵权风险、专利侵权风险、商标侵权风险和许可证冲突四类。

- a) 版权侵权由于不遵守开源许可协议造成,此类风险较易规避。
- b) 专利侵权由于开源代码中包含诸多软件专利,使用开源代码未得到软件专利权人的专利许可,从而导致专利侵权,此类风险较难规避。
- c) 商标侵权由于未经许可使用开源代码的商标造成,此类风险较易规避。
- d) 许可证冲突由于未遵守许可证的兼容性要求造成,此类风险较难规避。

A.3 开源持续性风险

开源持续性风险是指开源代码能否持续使用的风险。开源会因自然环境、外交、国际经贸等原因造成使用中断。

参 考 文 献

[1] GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南
[2] GB/T 36475—2018 软件产品分类
[3] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

中 华 人 民 共 和 国
国 家 标 准
网络安全技术 软件产品源代码安全
评价方法

GB/T 43848—2024

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址:www.spc.net.cn

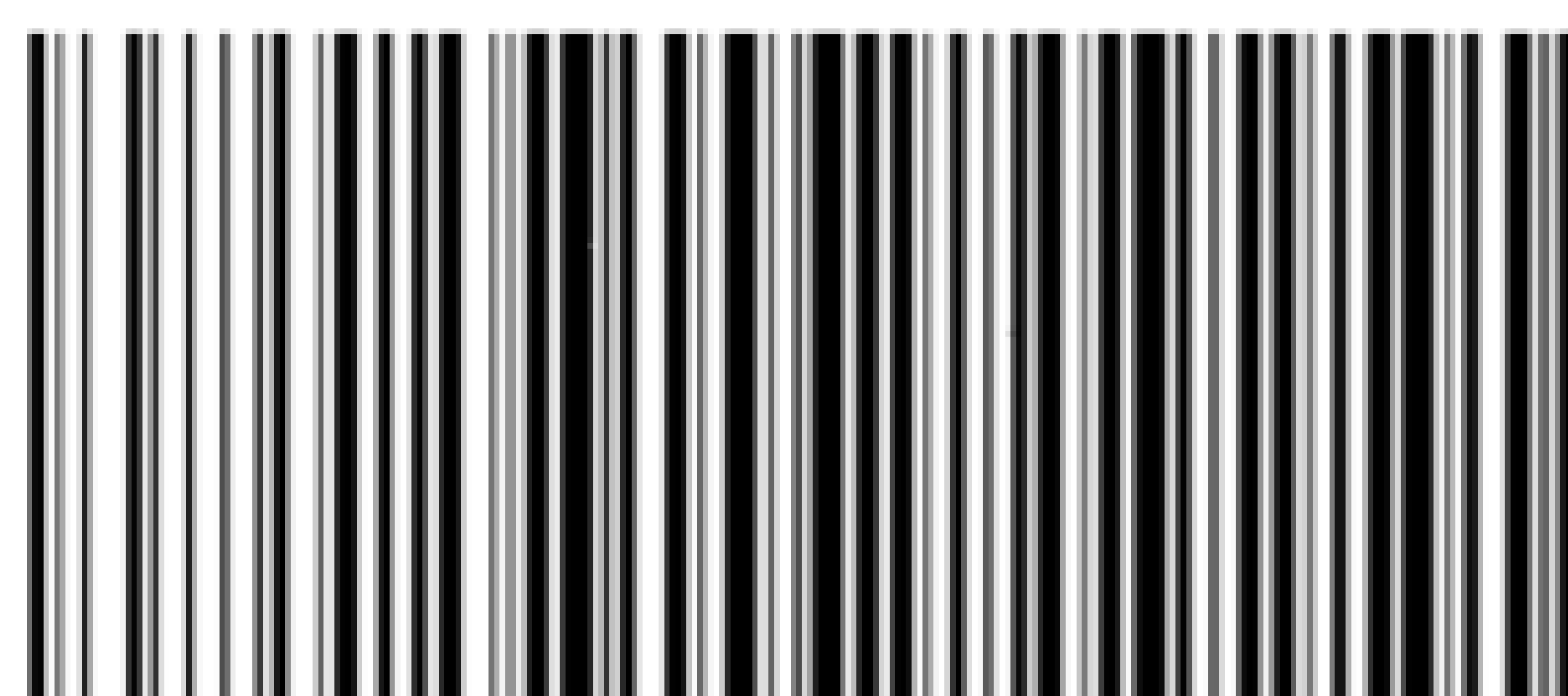
服务热线:400-168-0010

2024年4月第一版

*

书号:155066·1-75759

版权专有 侵权必究



GB/T 43848-2024